SPYWOLF

Security Audit Report

Completed on

August 11, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **Project-21** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

*Blacklist function detected

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> - SPYWOLF Team -

TABLE OF CONTENTS

Project-21

PROJECT DESCRIPTION

According to their whitepaper:

Project 21 builds a game based on a fantasy story and is launched on the Binance Smart Chain. Players need to create Laska Mecha and find companions to fight against A88 monsters, win and receive rewards from the game.

Release Date: Presale starts on August, 2022

Category: Play to earn (P2E)/NFT

CONTRACT INFO

Token Name
Project-21

Symbol
P21

Contract Address
0xD987Bf6F25d7ACd8ac6C5Cf3e92E753a69fbcdb0

Network
Binance Smart Chain

Language
Solidity

Deployment Date
August 10, 2022

Verified?
Yes

Total Supply
21,000,000

Status
Not launched

TAXES

Buy Tax
2%

Sell Tax
20%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of August 11, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

21,000

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	22978200 P21
Median Transfer Amount	21000000 P21
Average Transfer Amount	11489100 P21
First transfer date	2022-08-10
Last transfer date	2022-08-10
Days token transferred	1

SMART CONTRACT STATS

Calls Count	7
External calls	3
Internal calls	4
Transactions count	4
Uniq Callers	2
Days contract called	1
Last transaction time	2022-08-10 16:14:10 UTC
Created	2022-08-10 15:41:10 UTC
Create TX	0x0fdff5474af948319896a7e4105c77356a393e0cffebcea312f6f54a70c2c058
Creator	0xd5fd602838e26d67176ed78ca15b5e3793212121

FEATURED WALLETS

Owner address	0xd5fd602838e26d67176ed78ca15b5e3793212121
Liquidity address	0xb223f0d3549cc2248d1086bba873d97db6616161
Operations address	0xefd4f11605e8bba6785aa0dd37759f3281313131
Reserve address	0xedf555b486b06fd040105d64c5280f2f13515151
Rewards address	0x49b5a558442f45203e62b87d91366baba8414141
Token handler	0x07651624859050edc1ed4216e4b1cd2534559d5c
LP address	**Liquidity not added yet**

TOP 3 UNLOCKED WALLETS

1

90.6% Same as owner

0x42CB7024f7789aa35DeF41F2AE53e98284e9eBeF
*Contract unverified in BSCScan

9.4% 2

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell.

```
function manageRestrictedWallets(address[] calldata wallets,  bool restricted) external onlyOwner {
    for(uint256 i = 0; i < wallets.length; i++){
        restrictedWallets[wallets[i]] = restricted;
    }
}

function _transfer(address from, address to, uint256 amount) internal override {
...........
if(!earlyBuyPenaltyInEffect() && tradingActive){
    require(!restrictedWallets[from] || to == owner() || to == address(0xdead),
    "Bots cannot transfer tokens in or out except to owner or dead address.");
}
..........
}
```

⚠ Medium Risk

Owner can exclude address from fees and disable trading limitations.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}

function _transfer(address from, address to, uint256 amount) internal override {
...........
if(!tradingActive){
    require(_isExcludedFromFees[from] || _isExcludedFromFees[to], "Trading is not active.");
}
..........
}
```

⚠ Low Risk

Owner can change buy fees up to 2% and sell fees up to 25%.
Combined buy+sell=27%.

```
function updateBuyFees(uint256 _liquidityFee) external onlyOwner {
    buyLiquidityFee = _liquidityFee;
    buyTotalFees = buyLiquidityFee;
    require(buyTotalFees <= 2, "Must keep fees at 2% or less");
    emit UpdatedBuyFee(buyTotalFees);
}

function updateSellFees(uint256 _operationsFee, uint256 _liquidityFee,
uint256 _rewardsFee, uint256 _reserveFee) external onlyOwner {
    require(_operationsFee <= 1, "Exceeded max fee for operations");
    sellOperationsFee = _operationsFee;
    require(_liquidityFee <= 5, "Exceeded max fee for liquidity");
    sellLiquidityFee = _liquidityFee;
    require(_rewardsFee <= 25, "Exceeded max fee for rewards");
    sellRewardsFee = _rewardsFee;
    require(_reserveFee <= 3, "Exceeded max fee for reserve");
    sellReserveFee = _reserveFee;
    sellTotalFees = sellOperationsFee + sellLiquidityFee + sellRewardsFee + sellReserveFee;
    require(sellTotalFees <= 25, "Must keep fees at 25% or less");
    emit UpdatedSellFee(sellTotalFees);
}
```

Informational

Owner can withdraw any tokens from the contract.

```
function transferForeignToken(address _token, address _to) external onlyOwner returns (bool _sent) {
    require(_token != address(0), "_token address cannot be 0");
    require(_token != address(this) || !tradingActive, "Can't withdraw native tokens while trading is active");
    uint256 _contractBalance = IERC20(_token).balanceOf(address(this));
    _sent = IERC20(_token).transfer(_to, _contractBalance);
    emit TransferForeignToken(_token, _contractBalance);
}

// withdraw ETH if stuck or someone sends to the address
function withdrawStuckETH() external onlyOwner {
    bool success;
    (success,) = address(msg.sender).call{value: address(this).balance}("");
}
```

Owner can set max transaction limit, but can't lower it than 0.1% of total supply.

```
function updateMaxSellAmount(uint256 newNum) external onlyOwner {
    require(newNum >= (totalSupply() * 1 / 1000)/1e18, "Cannot set max sell amount lower than 0.1%");
    maxSellAmount = newNum * (10**18);
    emit UpdatedMaxSellAmount(maxSellAmount);
}
```

Owner can exclude address from transaction limits.

```
function excludeFromMaxTransaction(address updAds, bool isEx) external onlyOwner {
    if(!isEx){
        require(updAds != lpPair, "Cannot remove uniswap pair from max txn");
    }
    _isExcludedMaxTransactionAmount[updAds] = isEx;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

PROJECT-21

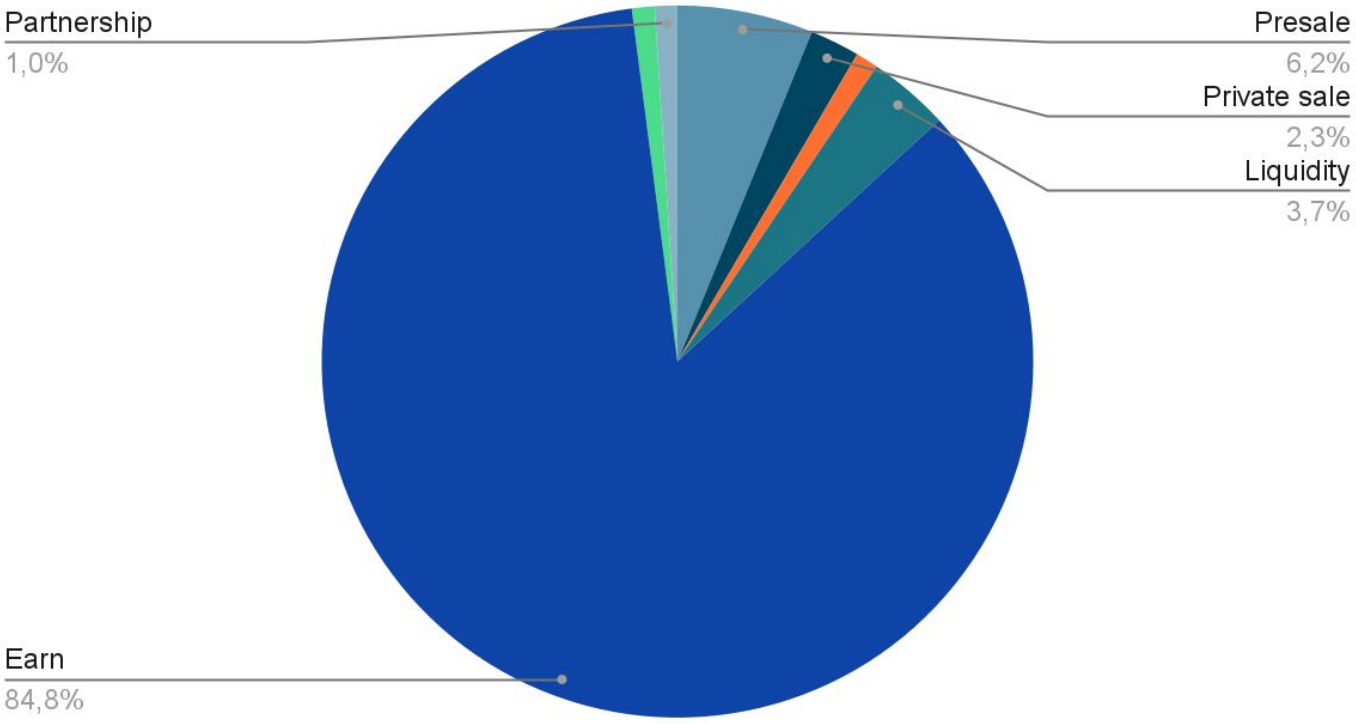
GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner can set a transaction limit, but cannot lower it than 0.1% of total supply

*The following tokenomics are based on the project's whitepaper and/or website:

- 6% - Public sale (*vested)
- 2.2% - Private sale (*vested)
- 3.6% - Liquidity
- 82.5% - Earn
- 1% - Marketing
- 1% - Dev (*vested)
- 1% - Partnership

Tokens distribution



*For more information about vesting periods, read project's whitepaper:
https://docs.project21.app/tokenomics

TOKENOMICS

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

WEBSITE

Website URL
https://project21.app/

Domain Registry
https://porkbun.com/

Domain Expiration
Expires on 2023-07-16

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

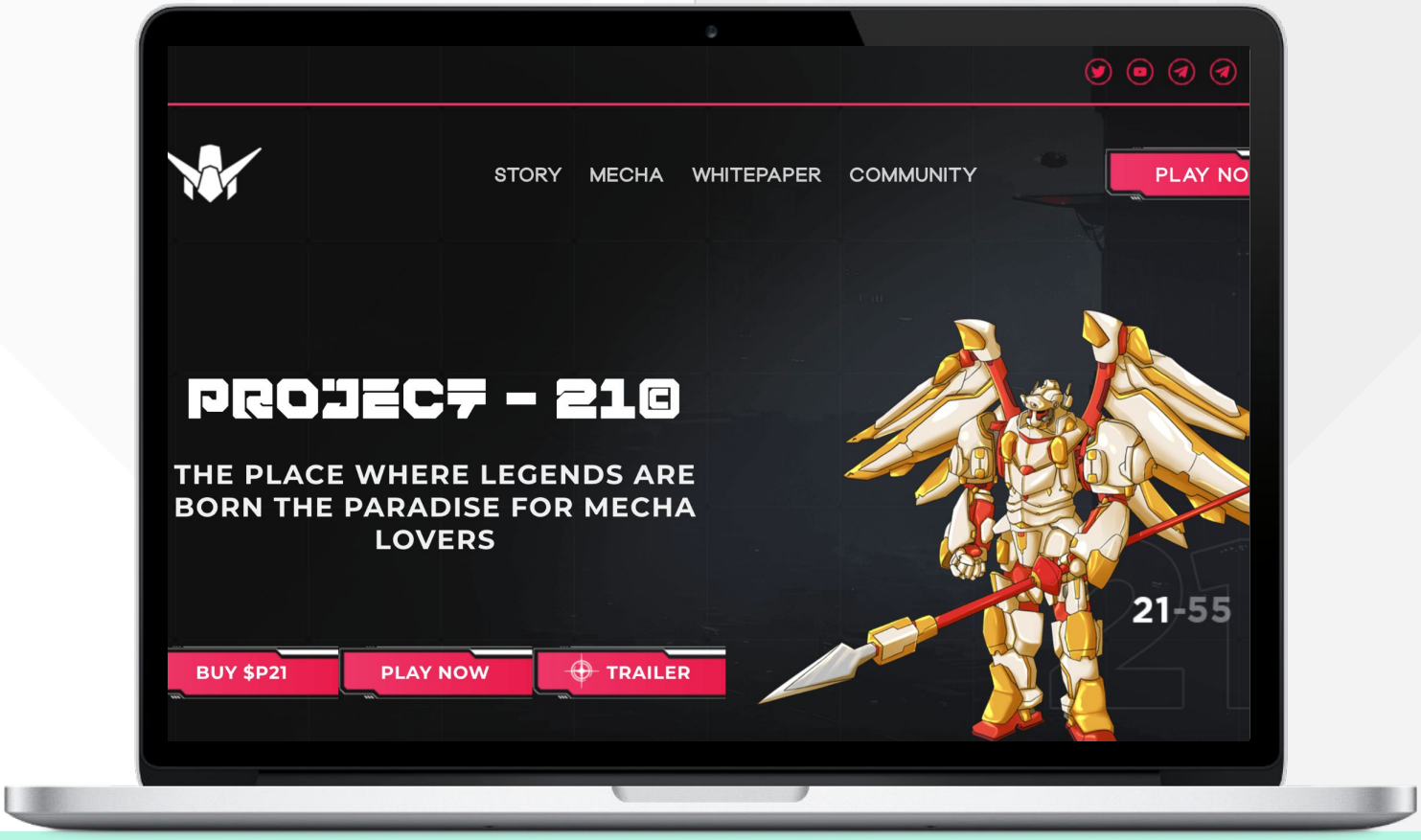
Design
Unique design, graphics and appropriate color scheme.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes



project21.app

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active with organic users' activity

Twitter

@Project21_bsc

- 4 343 followers
- Very Active
- Posts frequently

Discord

- Not available

Telegram

@TelegramUSERNAME

- 7 586 members
- Active users
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.